Implementación de un Servidor DNS Seguro basado en Pi-Hole utilizando un entorno virtualizado

Ernesto Sánchez, Daniel Arias Figueroa, Álvaro Ignacio Gamarra, José Nelson Mayorga

Universidad Nacional de Salta / Departamento de Informática / Facultad de Ciencias Exactas / Universidad Católica de Salta / Facultad de Ingeniería / Universidad Católica de Colombia
Av. Bolivia 5150, 3874255408 / Campus Castañares, 08105558227
esanchez@cidia.unsa.edu.ar, daaf@cidia.unsa.edu.ar, alvaroig@cidia.unsa.edu.ar, jnmayorga07@ucatolica.edu.co

Resumen

Desde su creación, el servicio de resolución de nombres proporcionado por el Sistema de Nombres de Dominio, se considera parte crítica para el funcionamiento de Internet. Esto lo convierte en el blanco de los más diversos ataques tales como redirección de consultas a sitios falsos, denegación de servicio, envenenamiento de cache, entre otros.

Como contramedida, se aunaron esfuerzos para el despliegue de extensiones de seguridad, que permitan autenticar, validar y hasta encriptar los mensajes intercambiados en el proceso de consulta/respuesta entre un cliente y un servidor DNS.

El presente trabajo, muestra una experiencia en el proceso de instalación y configuración de la solución de software Pi-Hole, para el despliegue de un Servidor DNS Resolver con extensiones de seguridad, en un ambiente virtualizado sobre VMWare y GNS3, posteriormente se realizaron capturas de tráfico de red, a fin de analizar funcionalidad y consumo de recursos.

Esta experiencia es de utilidad en la enseñanza del protocolo DNS en las asignaturas de grado y en los cursos de postgrado que organiza el Departamento de Informática de la Universidad Nacional de Salta.

Palabras clave: DNS Sumidero, DNSSEC, GNS3, Virtualización.

Contexto

La línea de investigación se encuentra apoyada por el C.I.D.I.A. (Centro de Investigación y Desarrollo en Informática Aplicada) que depende de la Facultad de Ciencias Exactas de la Universidad Nacional de Salta, por la Facultad de Ingeniería de la Universidad Católica de Salta y por el Gobierno de la Provincia de Salta, por lo tanto, se cuenta con toda la infraestructura disponible para esta investigación. El proyecto contará con el financiamiento del CIUNSa – Consejo de Investigación de la Universidad Nacional de Salta y el financiamiento del Consejo de Investigación de la Universidad Católica de Salta.

Introducción

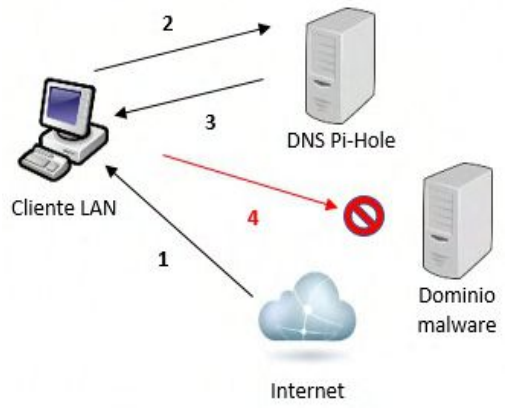
Desde su creación, el servicio de resolución de nombres proporcionado por el Sistema de Nombres de Dominio, se considera parte crítica para el funcionamiento de Internet, sin él, no sería posible el uso de aplicaciones de mensajería, redes sociales, comercio electrónico, redes privadas virtuales y tantas otras que hoy están presentes en Internet. Esto lo convierte en el blanco de los más diversos ataques tales como redirección de consultas a sitios falsos, denegación de servicio, envenenamiento de cache, entre otros. Como contramedida, se aunaron esfuerzos para el despliegue de extensiones de seguridad, que permitan autenticar, validar y encriptar los mensajes intercambiados en el proceso de consulta/respuesta entre un cliente y un servidor DNS.

La primera alternativa que logró un despliegue y adopción a escala global fue DNSSEC [1], sin embargo, este despliegue fue lento, debido a su complejidad y tareas de coordinación necesarias, dada la estructura jerárquica del sistema DNS.

Una vez superadas las etapas de pruebas y adopción, se desplegaron servicios para la resolución de nombres, proporcionados por Servidores Públicos tales como, Google DNS, OpenDNS, Cloudflare, Quad9, entre otros [2]. Tales Servidores proveen servicios extras como bloqueo de sitios con contenido malware, filtro de contenidos, optimización de tiempos de respuestas, así como aspectos de seguridad. Paralelamente, se desarrollaron soluciones de software open source, que automatizan y reducen los tiempos de implementación y despliegue de un Servidor DNS Resolver que hacen uso de los servicios proporcionados por los Servidores Públicos y brindan además un conjunto de herramientas, como el bloqueo de anuncios, gestión de "listas blancas" y "listas negras", extensiones de seguridad, todo administrable desde una interfaz web, que además permite monitorizar todo el tráfico de red intercambiado durante el proceso de resolución.

Una de estas soluciones de software es la que se presenta con el nombre de Pi-Hole, la cual se define como "*una aplicación para bloqueo de anuncios y rastreadores en Internet a nivel de red en Linux, que actúa como un sumidero de DNS, destinado para su uso en una red privada*" [3]

La siguiente figura muestra el principio de funcionamiento del servidor Pi-Hole.



El escenario anterior, presenta el caso en el que un Cliente conectado a una red LAN, solicita una página web que referencia a un dominio con contenido malware o recibe un mail conteniendo tal referencia. Se sigue la siguiente secuencia de pasos: [4]

1: Cliente LAN recibe mensaje que referencia a dominio con contenido malware.

2: Cliente LAN realiza con consulta DNS a Servidor DNS Local Pi-Hole.

3: Servidor Pi-Hole, identifica el dominio malicioso a partir de una "blacklist" y devuelve como respuesta una dirección IP loopback.

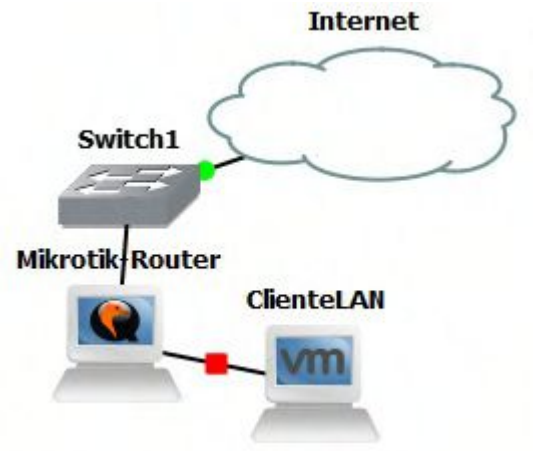
4: El cliente LAN no puede establecer conexión con el servidor con contenido malicioso.

Entorno de prueba utilizado.

A fin de poner a prueba los servicios proporcionados por el servidor Pi-Hole, se montó un entorno virtualizado utilizando las siguientes herramientas de software: [5]

- Plataforma de virtualización VMWare Workstation 15.
- Plataforma de simulación de redes GNS3 sobre Windows 10.
- Servidor Linux Ubuntu versión 16.04.6, virtualizado sobre VMWare, donde se configuró DNS Pi-Hole.

La topología creada sobre la plataforma GNS3, se muestra en la siguiente figura:



La siguiente tabla describe la configuración IP y funcionalidad de cada dispositivo:

Dispositivo	Dir. IP	Función
Nube		´Bridged a iface física
Mikrotik WAN	192.168.88.100	Enlace Internet
Mikrotik LAN	10.0.0.1	Gateway LAN
Cliente LAN	10.0.0.10	

El Servidor DNS se virtualizó sobre VMWare, con dirección IP: 192.168.88.20

Instalación y configuración DNS Pi-Hole

El proceso de instalación de la utilidad Pi-Hole se realiza en un único sencillo paso, utilizando un script disponible en el sitio oficial. Una vez instalado, se accede desde una interfaz web, a un completo panel de administración, que permite visualizar en tiempo real, cantidad de consultas procesadas, consultas bloqueadas y permitidas, entre otros datos estadísticos. Permite, además, la configuración de los servidores DNS públicos a utilizar y opciones adicionales de seguridad. [6]

Las opciones de configuración seleccionadas fueron; DNS público Quad9, y DNSSEC habilitado.

Líneas de Investigación, y Desarrollo

Los principales ejes temáticos que se están investigando son los siguientes:

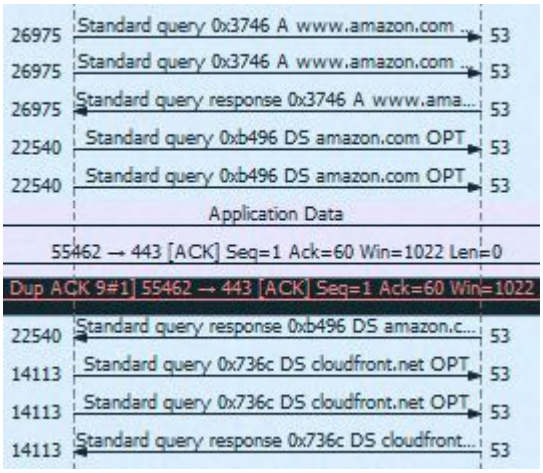
- Sistema de Nombres de Dominio.
- DNS Sumidero
- DNSSEC
- Simulación - Virtualización

Resultados Obtenidos/Esperados

Análisis de trazas consulta/respuesta DNSSEC.

Con el propósito de analizar la secuencia de los mensajes intercambiados en el proceso de resolución de una consulta DNS con extensiones de seguridad, se realizaron capturas de tráfico de red, utilizando la herramienta de software Wireshark, obteniendo los siguientes resultados.

A partir de la captura de una consulta al dominio www.amazon.com,se filtraron los mensajes correspondientes al protocolo DNSSEC, donde se observan los Registros de Recurso DS y RRSIG.



Ignorando los mensajes duplicados, la secuencia es la siguiente:

1) De cliente LAN a DNS Local Pi-Hole, consulta por dominio www.amazon.com.
2) De DNS Pi-Hole a DNS Público Quad9, consulta por dominio www.amazon.com. Se observa la presencia del bit DO activado, (Se aceptan Registros de Recursos DNSSEC).
3) Respuesta de DNS Público Quad9 a DNS Pi-Hole, indicando CNAME e IP.
4) En este punto, se inicia el proceso de verificación de la cadena de confianza, por lo que DNS Pi-Hole, realiza consulta de Registro DS (Delegation Signer) a DNS Público Quad9.
5) Servidor Quad9 responde con un Registro RRSIG, el cual contiene la firma sobre el dominio delegado, firmado por la entidad responsable del dominio .com.
6) Finalmente, el DNS Local responde al Cliente LAN, luego de haber comprobado la integridad y autenticidad de la respuesta recibida.

En conclusión, al habilitar las extensiones de seguridad, duplican la cantidad de mensajes y tiempos de respuesta, necesarios para el proceso de validación de la cadena de confianza DNSSEC, sin embargo, se consideran despreciables estos costos que aseguran una comunicación segura.

Análisis de bloqueo de anuncios

Con respecto a la funcionalidad principal del Servidor Pi-Hole, para el bloqueo de páginas con anuncios, se pudo observar que al recibir una consulta por un dominio que se encontrara en la "blacklist", Pi-Hole devuelve como respuesta un registro tipo A con dirección IP = 0.0.0.0.

A fin de conocer cuáles son los dominios bloqueados para el caso de la consulta por el dominio www.amazon.com, los dominios bloqueados son:

- fls-na.amazon.com
- s.amazon-adsystem.com
- c.amazon-adsystem.com

El listado anterior, así como otra información relevante a las consultas permitidas y bloqueadas, se obtienen a través de los reportes generados por Pi-Hole, accediendo desde su interfaz web.

En términos generales, se puede concluir que el despliegue de una arquitectura de Servidor DNS Resolver con extensiones de seguridad, requiere un mínimo de recursos, tanto de hardware como humanos. Así mismo, el proceso de instalación y puesta en marcha solo demanda unas cuantas horas.

Actualmente, existen dos implementaciones de esta arquitectura en entornos reales, una en el ámbito de la Universidad Nacional de Salta, y la otra en una dependencia del Gobierno de la Provincia de Salta. Como trabajo futuro, se pretende habilitar las opciones de extensiones de seguridad y realizar mediciones en cuanto a consumo de ancho de banda, tiempos de respuesta y consumo de recursos de procesamiento.

Formación de Recursos Humanos

El equipo de investigación se conforma con un director, dos docentes y un estudiante de intercambio de la Universidad Católica de Colombia con miras a en un futuro cercano firmar convenios de colaboración. Además se sumaran docentes de otras Universidades del país a través de convenios de cooperación que se firmarán oportunamente.

Bibliografía

[1] Tesis de Maestría, "Un estudio comparativo en Extensiones de Seguridad para el Sistema de nombres de Dominio", Mag. Ernesto Sánchez. http://sedici.unlp.edu.ar/handle/10915/63910.

[2] A List Of The Best Free and Public DNS Services https://makeawebsitehub.com/free-and-public-dns-services/

[3] Sitio oficial Pi-Hole. https://pi-hole.net/

[4] European Union Agency for Cyber Security. DNS Sinkhole. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/dns-sinkhole.

[5] Simulación de Redes con Mikrotik y GNS3. PCC en acción. MUM Argentina 2015. Ing. Álvaro Gamarra. https://mum.mikrotik.com/presentations/AR15/presentation_2878_1447676829.pdf.

[6] Pi Black Hole for Internet Advertisements. Rhythm Kr Dasgupta, JIS COLLEGE OF ENGINEERING. https://www.researchgate.net/publication/326319875